Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WC Docket No. 16-106
Broadband and Other Telecommunications	)	
Services	)	

PETITION FOR RECONSIDERATION OF COMPETITIVE CARRIERS ASSOCIATION

Steven K. Berry
President & CEO

Rebecca Murphy Thompson
EVP & General Counsel

Elizabeth Barket
Law & Regulatory Counsel

COMPETITIVE CARRIERS ASSOCIATION
805 15th Street NW, Suite 401
Washington, DC 20005
www.ccamobile.org

January 3, 2017

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106

PETITION FOR RECONSIDERATION OF COMPETITIVE CARRIERS ASSOCIATION

Competitive Carriers Association ("CCA")[1] respectfully submits this Petition for Reconsideration of the *Report and Order* adopted in the above-captioned proceeding ("*Report and Order*").[2]

I. INTRODUCTION & SUMMARY

The new privacy regime established by the Federal Communications Commission ("FCC" or "Commission") will undercut competition in the Internet ecosystem by saddling broadband Internet access service ("BIAS") providers with unparalleled, restrictive data use and sharing rules without the benefit of actually protecting consumers.[3] Further, the *Report and*

[1] CCA is the nation's leading association for competitive wireless providers and stakeholders across the United States. CCA's membership includes nearly 100 competitive wireless providers ranging from small, rural carriers serving fewer than 5,000 customers to regional and national providers serving millions of customers. CCA also represents approximately 200 associate members including vendors and suppliers that provide products and services throughout the mobile communications supply chain.

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, WC Docket No. 16-106, FCC 16-148 (rel. Nov. 2, 2016) ("*Report and Order*"). Note all comments and reply comments, unless marked otherwise, were filed in WC Docket No. 16-106 on May 28, 2016 and July 6, 2016 respectively.

[3] *See, e.g.*, Letter from Michael J. Jacobs, Vice President of Regulatory Affairs, ITTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, 2-3 (filed Oct. 21, 2016) ("ITTA *Ex Parte*") (explaining how "[w]eb browsing and app usage history are not considered sensitive by the FTC;" that "the FTC's Privacy Report endorsed an opt-out approach towards web browsing data used for behavioral advertising;" and that "[a]gainst the backdrop of the

Order does not provide appropriate relief for small providers who are unable to affordably shoulder the applicable compliance burdens. Accordingly, the Commission should reconsider implementing the *Report and Order* or, in the alternative, reconsider certain rules likely to overwhelm competitive carriers while failing to protect consumers.

At the outset, the Commission should reconsider the full *Report and Order* because it lacks legal authority to adopt it and because the Commission failed to establish a credible case that the rules will provide specific relief from concrete consumer harms. If the Commission will not revisit the rules entirely, the Commission should reconsider rules especially harmful to competitive carriers. First, the Commission should address rules that would disrupt competitive parity between BIAS providers and edge providers. Specifically, web browsing and application ("app") usage data should not be categorized as "sensitive customer PI," and the definitions of "customer proprietary information" ("PII") and customer proprietary network information ("CPNI") should be narrowed. In addition, as the Commission failed to comply with the Regulatory Flexibility Act ("RFA") in this proceeding and ignored the weight of record evidence regarding small carrier impact, the Commission should reconsider and expand the scope of its definition of "small provider" as well as the scope of relief provided to a small provider. Finally, the Commission should reconsider its data breach notification threshold to involve an intent element, so customers are only notified when a provider determines that financial or physical harm is reasonably likely to occur.

---

longstanding, embedded commercial practice of consumers benefiting from targeted advertising based on web browsing history, consumers do not have the same expectations of privacy in this context as they do with other categories of information").

II. THE COMMISSION SHOULD RECONSIDER THE ENTIRE *REPORT AND ORDER*

The Commission lacks the legal authority to adopt the *Report and Order* and has not proved that the rules would adequately address evidenced consumer harms, or even that harm exists. Accordingly, the whole *Report and Order* should be reconsidered.

a. The Commission Does Not Have the Authority to Adopt Privacy Rules for Information Beyond CPNI

The Commission chiefly predicates its authority to adopt the *Report and Order* on Section 222 of the Communications Act.[4] The Commission interprets Section 222 to permit authority over any "telecommunications carrier" providing a service consistent with that classification, as opposed to solely "telephone-specific" services.[5] Specifically, the Commission states that Section 222(a), by providing a duty to "protect the confidentiality" of "proprietary information," provides broad legal authority to enact information protection rules, which the Commission claims is not limited by other provisions of Section 222.[6] The Commission also predicates its authority on Section 222(c), Sections 201(b) and 202(a), Title III, and Section 706 of the Communications Act.[7]

CCA urges the Commission to reevaluate its authority to adopt the *Report and Order*, which unnecessarily expands the scope of information protected under the Section 222 voice

[4] *See Report and Order* ¶ 332.

[5] *See id.* ¶¶ 334-337; *see also id.* ¶ 350 ("…[W]e read Section 222(a) as imposing a broad duty that can and must be read in harmony with the more specific mandates set forth elsewhere in the statute").

[6] *See id.* ¶¶ 343-344.

[7] *See id.* ¶¶ 364-372.

regime.[8] Considering the structure and legislative history of Section 222, it is not reasonable to assume Section 222(a) was intended to provide the Commission with broader power over information exchanged on the Internet, a materially different information environment.[9] The use of "proprietary information" in 222(a)[10] should be understood to encompass only the categories of information described elsewhere in Section 222, such as carrier "proprietary information" in 222(b) and "CPNI" used in section 222(c).[11] The "unattached" mention of equipment manufacturers in Section 222(a) does not, as the Commission posits, support the argument that

[8] *See* CCA Comments at 15-16. CCA supports arguments on record disproving the Commission's authority to adopt the *Report and Order* on the strength of Sections 201 and 202, or Sections 705 or 706 of the Act. *See, e.g.,* CTIA Reply Comments at 26-32.

[9] *See* H.R. Conf. Rep. No. 458, 104th Cong., 2d Sess. 204 (1996) (Joint Explanatory Statement of the Committee on Conference) (explaining that subsection 222(a) is limited to telecommunications carriers' responsibility to "protect the confidentiality of proprietary information," and further explaining that subsection 222(c) "limits" telecommunications carriers' use, disclosure, or access to CPNI except as explicitly provided in the statute or through customer approval); *see also* CTIA Comments at 28-29 (when the full Congress passed Section 222, it chose not to include language that would have broadened the scope of customers' "proprietary information," and instead passed a bill that limited the scope of Section 222 to CPNI).

[10] *See* 47 U.S.C. 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier").

[11] *See* CCA Comments at 15 ("Section 222(a) does not provide independent authority to expand the type of information protected by the statute. Section 222 clearly sets forth the type of companies to be covered, the type of information to be protected and the various exceptions that Congress decided were appropriate. Section 222(a) also sets forth a 'general' duty, focusing on which entities would be responsible to protect CPNI: all 'telecommunications carriers.' Sections 222(b) and 222(c) detail *when and how* that general duty is to be exercised. Section 222(c) provides the Commission with the authority to regulate the security of the data, specifically limiting the type of proprietary information that is required to be protected under the statute to 'consumer proprietary network information.' Section 222(h) explicitly defines this term to be limited to the 'quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service' as well as 'information contained in the bills pertaining to telephone exchange service or telephone toll service. . .'").

this provision is a standalone grant of power with respect to broadband providers.[12] If anything, that language suggests that the Commission's authority is in fact limited as described in 222(c). The text of Section 222 speaks only and specifically of "call[s]," "call location information," "local exchange carrier[s]," "IP-enabled voice service," "telephone exchange service," "telephone toll service" and "telemarketing."[13] Further, nothing in Section 222 allows the Commission to pass broad data security mechanisms.[14] Regulatory overreach of this magnitude will be enormously costly for stakeholders without clear consumer benefits, and should be reconsidered.

Indeed, this drastic regulatory overreach is not in the public interest. Vast new regulations—which touch important aspects of a carrier's day-to-day operations, services, as well as long and short-term initiatives—should be on a solid legal foundation to provide certainty for telecommunications stakeholders. Without that certainty, carriers are forced to make resource-intensive administrative and systematic changes per rules unlikely to withstand legal review. This uncertainty will destabilize competitive carriers' businesses. Increasing carriers' compliance costs ultimately will raise customer service costs, and inconsistent changes in privacy regimes will confuse consumers about how their information is handled; this will have the effect of decreasing consumer choice and engagement. The Commission should therefore reconsider its legal basis for, and withdraw, the entire *Report and Order*.

[12] *See Report and Order* ¶ 346.

[13] *Id.*

[14] *See supra* note 9.

b. The Commission Should Reconsider the *Report and Order* Until a Credible Case for Consumer Harm is Made

The discussion of consumer harm in the *Report and Order* relies on statistics implying consumer anxiety about the way information is shared online. For example, the "Commission has found, if 'consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand,'" and "fear of privacy violations chills online activity, to the point where privacy concerns prevented 45 percent of online households from conducting financial transactions, buying goods or services, or posting on social networks."[15] The Commission also asserts that requiring providers to secure "opt-in" approval for use and sharing of information designated as sensitive customer PI "materially advances" enabling customers to "avoid unwarranted and unexpected" use of that information.[16]

While consumers are rightly concerned about online privacy, the Commission provides no concrete facts or evidence to prove that BIAS providers are at the root of those concerns. More specifically, the Commission has not proved that its adopted policies will prevent harm to consumers, and evidence that providers' targeted advertising practices are harmful is notably absent from the *Report and Order*.[17] Similarly egregious, the actual rules adopted bear little

---

[15] *Report and Order* ¶ 379.

[16] *Id.* ¶ 383.

[17] The vast majority of small providers do not use consumer data for purposes outside of providing BIAS. *See, e.g.*, Letter from Patricia Cave, Director, Government Affairs, WTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2-3 (filed Aug. 22, 2016) ("WTA Ex Parte"); *see also* RWA Reply Comments at 2 ("[U]nlike large or nationwide BIAS providers, [our] members do not generally collect, store, analyze, and exploit [CPNI]"); WTA Comments at 19 ("Small BIAS providers also do not engage in the collection and retention of sensitive consumer information to the extent that other industry participants that are subject to FTC enforcement do."); CCA Comments at 33 ("[M]any CCA carrier members that fall under

resemblance to the FTC regime—which is far more likely to reflect what consumers actually expect online.[18]

Nor has the Commission appropriately balanced compliance burdens with consumer protections. In fact, at no point in the *NPRM* or the *Report and Order* did the Commission conduct a cost-benefit analysis of the proposed or adopted rules,[19] specifically regarding what costs would befall small entities.[20] It seems greater harm will come from destabilizing competitive carriers, or increasing service costs that could translate into higher service costs, than from failing to effectuate the rules in the *Report and Order*. These rules, then, should be reconsidered in their entirety until a credible case for consumer protection is made.

CCA's proposed definition of small provider do not share customer information with third parties for advertising purposes."); NTCA Comments at 1 ("As a general matter . . . NTCA members do not broker their customers' information."); ACA Comments at 5 (explaining that "ACA members generally do not use their customers' information for purposes requiring opt-in consent—often because they lack the incentive or resources to do so").

[18] *See* Comments of Progressive Policy Institute, WC Docket No. 16-106 (filed May 27, 2016) (submitting a recent survey by Public Opinion Strategies and Peter D. Hart, stating that 94% of Internet users agree that "[a]ll companies collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it."). *See also* CCA Reply Comments at 20 ("Even as 91% of adults indeed agree or strongly agree that consumers have lost control of how personal information is collected, 'most Americans who are making decisions about sharing their information in return for a product, service or other benefit' say 'the context and conditions of the transactions' dictate their decisions, including the 'terms of the deal; the circumstances of their lives; whether they consider the company or organization involved to be trustworthy; [and] what happens to their data after they are collected…'), *citing* Lee Raine, *The state of privacy in America; What we learned,* Pew Research Center (Jan. 20, 2016), *available at* http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.

[19] *See Report and Order,* Dissent of Commissioner O'Rielly, pg. 218 ("Dissent of Commissioner O'Rielly").

[20] *See, infra,* Section III.c.

III. IN THE ALTERNATIVE, THE COMMISSION SHOULD RECONSIDER OVER-BURDENSOME RULES THAT PLACE BIAS PROVIDERS AT A COMPETITIVE DISADVANTAGE WITHIN THE INTERNET ECOSYSTEM

In the event that the Commission does not rescind the *Report and Order* for the foregoing reasons, the FCC should reconsider a number of rules which will harm competitive carriers without materially addressing consumer privacy concerns.[21] The Commission should eliminate web browsing data and app usage history from its definition of "sensitive customer PI," exclude advertising indicators from PII, limit the new definition of CPNI, expand the scope of relief afforded to small providers, and more reasonably craft data breach notification rules.

a. The Commission Should Not View Web Browsing Data and App Use Data As "Sensitive Customer PI"

The *Report and Order* adopted a definition of "customer proprietary information" ("customer PI") that encompasses any information a carrier acquires in connection with its provision of telecommunications service comprising three non-exclusive buckets of information: "individually identifiable customer proprietary network information" ("CPNI"), PII, and "content of communications."[22] The Commission broadly expanded the definition of CPNI to include many if not all components of an Internet protocol packet.[23] PII is defined as "any

---

[21] *See Report and Order,* Dissent of Commissioner Pai at pg. 200 ("Dissent of Commissioner Pai") (urging the Commission to hew more closely to the FTC's successful, technology-neutral framework).

[22] § 64.2002(f); *Report and Order* ¶ 46 ("[W]e import the statutory definition of customer proprietary network information (CPNI) into our implementing rules, and define customer proprietary information (customer PI) as including individually identifiable CPNI, personally identifiable information (PII), and content of communications. We recognize that these categories are not mutually exclusive, but taken together they identify the types of confidential customer information BIAS providers and other telecommunications carriers may collect or access in connection with their provision of service").

[23] *Report and Order* ¶ 53-4; *see id.* ¶ 48 ("We interpret the phrase 'made available to the carrier by the customer solely by virtue of the carrier-customer relationship' in Section 222(h)(1)(A) to include any information falling within a CPNI category that the BIAS provider collects or accesses in connection with the provision of BIAS. This includes information that may also be

information that is linked or reasonably linkable to an individual or device."[24] Providers must obtain a customer's opt-in consent before using or sharing sensitive customer PI,[25] and further must "offer their customers the ability to opt out of the use and sharing of non-sensitive customer information."[26] Sensitive customer PI includes, "at minimum, financial information; health information; Social Security numbers; precise geo-location information; information pertaining to children; content of communications; call detail information; and a customer's web browsing history, application usage history, and their functional equivalents."[27]

These rules prevent parity between BIAS providers and edge providers, and consistency with the FTC regime. As such, the Commission should reconsider its approach to the definition of "sensitive" information to allow reasonable, competitive use of web browsing history and app use history.

First, BIAS providers are not uniquely-situated "gatekeepers" meriting the restrictive rules adopted, and the Commission is wrong to rely on this premise.[28] In the *Report and Order*, the Commission ignores the vast body of evidence on record suggesting that edge providers are far more active and able data collectors than BIAS providers.[29] Consider Oracle's example of

---

available to other entities"); *id.* ¶ 53 (CPNI includes IP addresses and domain name information, application header, application payload, and customer premises equipment and device information).

[24] *Id.* ¶ 89 ("Information is linked or reasonably linkable to an individual or device if it can reasonably be used on its own, in context, or in combination to identify an individual or device, or to logically associate with other information about a specific individual or device").

[25] *Id.* ¶ 177; *see* § 64.2002(c).

[26] *Id.* ¶ 172; *see* § 64.2002(b).

[27] *Id.* ¶ 177.

[28] *See* Dissent of Commissioner Pai at 210.

[29] *See, e.g.*, Reply Comments of CCA at 27-30 (describing extensive data-gathering and analysis practices of Amazon, Apple, Facebook, and the Washington Post).

the treasure trove of data an Android device sends back to Google every time a consumer "wakes" the device.[30] In addition, "Google's recent decision to link its DoubleClick data into its profiles exponentially expands Google's ability to aggregate specific consumer data that is exceedingly more pervasive than other technology companies."[31] These examples as well as many others on record suggest edge providers have the proverbial "edge" when it comes to collecting and mobilizing consumer data, not BIAS providers.

Worse, the Commission has not given enough weight to consumer-friendly methods for sifting through web browsing and app usage data. The Commission argues that parsing customer data into "sensitive and non-sensitive categories is a fundamentally fraught exercise,"[32] and it rejects blacklisting and whitelisting, which have been shown to be reasonable solutions to simplifying data management.[33] Further, as CCA has discussed, ambiguity as to whether certain website addresses or apps implicate traditionally "sensitive" categories like health and financial information does not justify "adopting an overly-broad rule that imposes uneven regulations and

---

[30] *See* Petition for Reconsideration of Oracle, WC Docket No. 16-106, 6 (filed Dec. 21, 2016) ("*Oracle PFR*") ("the device sends and receives over 35 data requests. Among these requests, the device transmits to Google its (i) location, (ii) Google Play ID, and (iii) Mobile ID").

[31] *See* "*Oracle PFR* at 5-7; *see also* Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech, et al., Working Paper, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, WC Docket No. 16-106, at 24-25 (filed May 27, 2016) ("Swire Paper"); Electronic Privacy Information Center ("EPIC") Comments at 16.

[32] *Report and Order* ¶ 187-188.

[33] *See* Letter from James J.R. Talbot, Executive Director and Senior Legal Counsel, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, 3 (filed Oct. 17, 2016) ("Like any other Internet company, a broadband provider can avoid the use of sensitive information by categorizing website and app usage based on standard industry interest categories established by the Interactive Advertising Bureau ('IAB') and other leading industry associations. This process involves correlating non-content web address or app information (e.g., visit to a sports website) with a pre-established "white list" of permissible interest categories (e.g., sports lover) available from the IAB. The list of interest categories can be refined as needed to exclude any sensitive categories.") ("AT&T Letter").

causes significant customer confusion."[34] The Commission also appears to have ignored data suggesting consumer concern about online data is dependent on context, and limited to a few pieces of common-sense "sensitive" information like Social Security numbers.[35] Indeed the Commission's privacy regime, which is inconsistent with the FTC privacy regime that applies to all other entities in the Internet ecosystem, will confuse consumers. This is particularly the case with respect to the opt-in regime for web browsing and app usage data. Such confusion will unduly cultivate a negative impression of their provider.[36]

As the FCC's privacy rules do not apply to edge providers, carriers who can afford to do so will simply purchase consumer information from those third parties. Therefore, the

---

[34] *See id.* *See also* Letter from Rebecca Murphy Thompson, EVP & General Counsel, to Marlene H. Dortch, Secretary, FCC, Docket No. 16-106, 5 (filed Oct. 13, 2016) (advocating before the Wireline Competition Bureau for a two-year compliance deadline for small providers, along with other targeted relief for small providers) ("CCA Small Provider *Ex Parte*"). Further, whitelisting is, "for the most part, straightforward and technologically feasible to implement," and "specified 'sensitive' categories will serve as a building block as the meaning of sensitive information evolves over time." *See* FTC Comments at 22 n. 91; *see also* Sydney M. White, Counsel, Internet Commerce Coalition to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, 2-3 (filed Oct. 18, 2016) (describing how ISPs and Internet companies use a combination of "white lists" and "black lists" that "isolate and exclude data categorized as sensitive by the FTC"); Mike Signorelli, for American Association of Advertising Agencies, to Marlene H. Dortch, Secretary, FCC, Docket No. 16-106, 2 (filed Oct. 21, 2016) ("[C]ompanies across the Internet, including ISPs, have for decades used a combination of administrative and technical controls to limit the use of sensitive data for marketing and advertising purposes, absent consumer consent. These practices were developed to comply with the FTC's privacy framework and the self-regulatory program administered by the DAA").

[35] *See* CCA Reply Comments at 20-21 ("'[M]ost Americans who are making decisions about sharing their information in return for a product, service or other benefit' say 'the context and conditions of the transactions' dictate their decisions, including the 'terms of the deal; the circumstances of their lives; whether they consider the company or organization involved to be trustworthy; [and] what happens to their data after they are collected.' For example, 90% of adults consider Social Security numbers to be 'very sensitive,' and 50% of adults also consider information about their health and medications, the content of their email and phone conversations, or details of their 'physical location over time' to be 'very sensitive.' On the other hand, only 8% found information about 'basic purchasing habits' to be 'very sensitive'").

[36] *See* CCA Reply Comments at 27.

Commission has merely raised the cost to compete in the Internet ecosystem,[37] where those with the most effective use of data resources tend to reap the highest rewards in the fast-growing digital advertising marketplace. Indeed, the Commission will stifle innovation for competitive carriers.[38] Because these rules create unhelpful disruption and confusion for consumers and competitors alike, the aforementioned rules should be reconsidered.[39]

b. The Commission Should Refine Other Overbroad Provisions

The Commission should narrow the scope of information covered by the Commission's definition of "customer PI" to exclude information that is highly unlikely to harm consumers if shared, consistent with the FTC regime. These common-sense changes will make the *Report and*

[37] *See Dissent of Commissioner O'Rielly* at pg. 216-217.

[38] *See* CCA Reply Comments at 31-33, *citing* The Brattle Group, *Mobile Broadband Spectrum: A Vital Resource for the U.S. Economy* (May 11, 2015), *available at* http://www.ctia.org/docs/default-source/default-document- library/brattle_spectrum_051115.pdf ("Brattle Group Study").

[39] The Commission also should allow use of sensitive data for first-party marketing, as long as the company's business model is not designed to target customers based on that sensitive data. *See* FTC 2012 Privacy Report at 47-48. The FTC has recognized that requiring express consent for first-party marketing should be limited to instances "a company's business model is designed to target consumers based on sensitive data – including data about children, financial and health information, Social Security numbers, and certain geolocation data." *Id.* at 47. Conversely, "the risks to consumers may not justify the potential burdens on general audience businesses that incidentally collect and use sensitive information." *Id.* at 47-48. It is entirely consistent with the context of a provider's relationship with their customers to collect and use consumer data, and indeed consumers increasingly expect tailored services. Sprint Comments at 9, *citing* Peter Dahlstrom & David Edelman, *The Coming Era of 'On-Demand' Marketing*, MCKINSEY QUARTERLY (Apr. 2013), *available at* http://www.mckinsey.com/business-functions/marketing-and-sales/ourinsights/the-coming-era-of-on-demand-marketing (forecasting increase in customer "expect[ations] [that] all data stored about them [will] be targeted precisely to their needs or used to personalize what they experience"); Sprint Comments at 21 ("Indeed, evidence increasingly shows that consumers willingly disclose such information to obtain a variety of benefits, including personalization, free services, and useful advertisements"). The FTC has recognized more broadly that use of customer information for first-party marketing can be made on the basis of inferred consent. *See* FTC 2012 Privacy Report at 39-40.

Order far easier for BIAS providers to implement without compromising their customers' service expectations.

1. The Definition of "CPNI" Should be Abbreviated

The definition of CPNI appearing in the *Report and Order* is overbroad.[40] As IP addresses, domain names, application header information and MAC addresses are simply tools used to direct online traffic, they are not proprietary and thus should be struck from the *Report and Order* definition of CPNI. Similarly, the type of service a customer receives should not be considered CPNI. Although only "precise geolocation information" appears in the *Report and Order* definition of "sensitive" information, the Commission later suggests it has a broader definition in mind.[41] The Commission should therefore clarify its intent to exclude information that is not "precise geolocation" information, and eliminate the other aforementioned items from the definition of CPNI.

2. Advertising Identifiers Should Not Be Considered Customer Proprietary Information

The FCC should reconsider the scope of the definition of customer PI to exclude so-called PII including persistent online or unique advertising identifiers,[42] which cannot be

---

[40] CCA Comments at 12-13.

[41] *See Report and Order* ¶¶ 65-66 (reaffirming that geo-location is CPNI including "many types of data—either individually or in combination—[used] to locate a customer, including but not limited to GPS, address of service, nearby Wi-Fi networks, nearby cell towers, and radio-frequency beacons" when made available to the BIAS provider by virtue of the carrier-customer relationship).

[42] *See id.* ¶ 93 ("We find that examples of PII include, but are not limited to: name; Social Security number; date of birth; mother's maiden name; government-issued identifiers [e.g., driver's license number]; physical address; email address or other online contact information;[42] phone numbers; MAC addresses or other unique device identifiers; IP addresses; and persistent online or unique advertising identifiers. Several of these data elements may also be CPNI").

associated with a named individual without additional linking information.[43] Standing alone, these "randomly generated numbers associated" with a consumer's device do not identify a consumer by name, physical address, or any other information traditionally considered PII and can be regenerated by a consumer, which generates a new number, making it much less likely that this type of number could be relied upon to identify an individual person.[44] It is thus highly unlikely that access to an advertising identifier in isolation could cause harm to a consumer. As such, protecting advertising identifiers as PII will waste provider resources without providing a privacy benefit to consumers. Therefore, the Commission should focus its rules to capture information that is "linked or reasonably linkable" to a consumer by specifically identifying personal information, such as pairing a device identifier with a consumer's name or address.

c. The Commission Should Expand the Small Provider Exemption

In the *Report and Order*, the Commission provided a mere one-year compliance extension of the notice and choice provisions for providers serving 100,000 subscribers or less.[45] This was the only relief afforded to providers defined as "small."

The Commission should reconsider its definition of "small provider" to align with the Small Business Administration ("SBA") definition or one supported by Congress and allow all providers additional time, especially smaller providers, to comply with all new rules adopted in the *Report and Order*.[46]

---

[43] *See* National Advertising Initiative, *Frequently Asked Questions*, *available at* https://www.networkadvertising.org/faq; *see also* Android, *Working with Advertising IDs*, *available at* https://developer.android.com/training/articles/user-data-ids.html#working_with_advertising_ids.

[44] *Id.*

[45] *Report and Order* ¶ 320-322.

[46] CCA Small Provider *Ex Parte*; *see also See* Letter from Rebecca Murphy Thompson, EVP & General Counsel, to Marlene H. Dortch, Secretary, FCC, Docket No. 16-106 (filed Oct. 19,

Despite the fact that the SBA has defined a small provider as serving 500,000 or fewer consumers or with 1,500 or fewer employees, and Congress has identified similar small provider thresholds,[47] the FCC unilaterally, without support in the record, established a new small carrier threshold for its enhanced transparency rules. This threshold, 100,000 or fewer connections,[48] far underestimates the type of carrier who will have trouble affordably and quickly complying with many of the rules. Therefore, the Commission should reconsider the adopted definition of small provider, one serving 100,000 or fewer connections, to a provider serving 250,000 subscribers or less, to reflect Congress's bipartisan, bicameral support for the Small Business Broadband Deployment Act, or should adopt the SBA definition: those providers serving 500,000 subscribers or less, or with 1,500 or fewer employees.

2016) (discussing expanded relief for small providers with, in separate meetings, staff of Chairman Wheeler; staff of Commissioner Clyburn; staff of Commissioner Pai; and staff of Commissioner O'Rielly).

[47] CONFERENCE REPORT, TELECOMMUNICATIONS ACT OF 1996, S. DOC. NO. 104-230 at 204 (Feb. 1, 1996) (to Accompany S. 652), *available at* ftp://ftp.fcc.gov/pub/Bureaus/OSEC/library/legislative_histories/1749.pdf ("Section 222(d) allows the Commission to exempt from its requirements of subsection (b) carriers with fewer than 500,000 access lines, if the Commission determines either that such an exemption is in the public interest or that compliance would impose an undue burden"). The House of Representatives and the Senate have each, with respect to exempting small providers from the enhanced transparency rules established by the *2015 Open Internet Order*, passed respective versions of the Small Business Broadband Deployment Act (the "Act"), which defines small providers as those serving 250,000 subscribers or less. *See* Small Business Broadband Deployment Act, H.R. 4596, 114th Cong. (2016); *see also* H. Energy and Commerce Comm., 114th Cong., *Text: H.R. 4596, The Small Business Broadband Deployment Act* (Mar. 14, 2016), https://www.congress.gov/bill/114th-congress/house-bill/4596/text?q=%7B"search"%3A%5B"HR4596"%5D%7D&resultIndex=1; *see also* Small Business Broadband Deployment Act, S.2283, 114th Cong., *Text: S.2283, Small Business Broadband Deployment Act*, https://www.congress.gov/bill/114th-congress/senate-bill/2283/text.

[48] *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order, 30 FCC Rcd 14162, ¶ 4 (CGB 2015) ("*Small Provider Exemption Report and Order*").

Additionally, the scope of the small provider exemption should be reconsidered as the FCC did not comply with its obligations under the RFA,[49] which requires a detailed examination of how the proposed rules could impact small providers. Congress passed the RFA because "the failure to recognize differences in the scale and resources of regulated entities has in numerous instances adversely affected competition in the marketplace, discouraged innovation and restricted improvements in productivity."[50] Specifically, the Initial Regulatory Flexibility Analysis ("IRFA") accompanying the *Privacy NPRM* did not describe and assess the economic impact of the Commission's proposals on small entities, nor did the IRFA discuss alternative rules that may ameliorate burdens.[51] Although the Commission estimated the number of small BIAS providers that may be impacted by the rules, the Commission did not provide "a quantifiable or numerical description of the effects of a proposed rule or alternatives to the proposed, or more general descriptive statements if quantification is not practicable or reliable."[52] The small business expert entity, SBA, stated outright that "the FCC failed to comply with the RFA's requirement to quantify or describe the economic impact that its proposed regulations might have on small entities," a sentiment echoed by the bipartisan leadership of the House Small Business Committee.[53] In response, the Commission's only

[49] 5 U.S.C. §§ 601-12.

[50] Regulatory Flexibility Act, Congressional Findings and Declaration of Purpose (a)(3).

[51] 5 U.S.C. § 603.

[52] *Id.* § 607; *see id.* at § 602 (certain requirements to publish small business impacts in the Federal Register).

[53] *See Ex Parte* Letter from Darryl L. DePriest, Chief Counsel for Advocacy, SBA Office of Advocacy, and Jamie Belcore Saloom, Assistant Chief Counsel, SBA Office of Advocacy, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 2, 4 (filed June 27, 2016) ; *see also* Letter from Steve Chabot, Chairman, U.S. House of Representatives Committee on Small Business, and Nydia Velazquez, Ranking Member, U.S. House of Representatives Committee on Small Business, to Hon. Tom Wheeler, Chairman, FCC (Aug. 25, 2016) (decrying the

defense was its subsequent enactment of "numerous measures in [the *Report and Order*] to alleviate burdens for small providers."[54] The lack of a good faith effort to comply with the RFA sets a poor precedent of neglecting the needs of vulnerable small businesses, and therefore cuts against the public interest.

Further, the new privacy rules will create legal, network and administrative requirements with which all carriers must comply. The need for a two-year compliance window for small carriers also is amply supported by the record.[55] While smaller carriers will be hardest hit, the FCC should provide all carriers, large and small, additional time to implement new complex and costly privacy regulations.[56]

Commission's failure to comply with the RFA, and asking the Commission to make public a review of the impact that the proposed privacy riles would have on small providers).

[54] *Report and Order,* Appendix B, Final Regulatory Flexibility Analysis ¶ 12.

[55] *See* CCA Small Provider *Ex Parte* at 1 ("As CCA and many others have explained, small carriers face a daunting administrative and resource challenge when faced with the need to alter notification procedures, information gathering and storage protocols, data security systems and training, and seek legal counsel, when possible, to ensure compliance. A longer, uniform time period to comply with newly adopted privacy rules will afford small carriers time to implement necessary changes without any interruption or degradation of service"); *see also,* WISPA Comments at 27-28 (seeking a two-year extension for all the Commission rules); Letter from Michael J. Jacobs, Vice President of Regulatory Affairs, ITTA, to Marlene H. Dortch, WC Docket No. 16-106, 3 (filed Sept. 30, 2016) (same); *See* WISPA Comments at 28 ("This additional time will enable small providers to assess their obligations, budget for lawyers, consultants, train personnel, and establish internal systems to ensure compliance.") *see also* ACA Comments at 8 (arguing that "very few of these [small] providers have in-house technical or compliance personnel with extensive expertise in privacy and data security compliance. Some are forced to outsource some of their security functions to outside vendors at a significant cost"); RWA Reply at 7 ("If the Commission declines to adopt these broader exemptions, RWA urges the adoption of a 24-month extended compliance deadline for small providers.")

[56] *See, e.g.,* Letter from Michelle R. Rosenthal, Senior Corporate Counsel, T-Mobile, to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106, 1-2 & n.1 (filed Sept. 13, 2016) (listing the actions companies must undertake to implement the new rules, including "analyzing rules for changes and requirements; discussing with various segments of our business; updating privacy, data security, and other policies; updating programs and certifications; updating tools to track and administer compliance programs; developing and giving training updates to employees and vendors; working with businesses, information technology, and security to update systems and

The Commission forgets that these small businesses are comprised of members of the public. Rural and regional carriers are important to their communities, providing solid jobs, innovation, and important public safety capabilities and enhancements. Therefore, it is in the public interest to expand the scope of the definition of "small provider" to one supported by Congress or already approved by the SBA, and to create a two-year extension from all rules set by the *Report and Order*.

d. Breach Notification Rules Should be Grounded in Actual, Identifiable Harms to Consumers

Under the *Report and Order*, a provider is required to notify customers of a breach "no later than 30 days after the carrier reasonably determines that a breach has occurred… unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach."[57] The Commission clarified that the adopted "harm-based trigger" encompasses "financial, physical, and emotional harm,"[58] as well as "reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal

---

practices; updating customer facing information and user interfaces; updating customer care and retail practices and providing training; reviewing and updating vendor contracts; and developing and designing reporting mechanisms, among other things). *See also* Letter from Catherine M. Hilke, Assistant General Counsel, Verizon, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, 1 (filed Sept. 23, 2016) ("Once rules are adopted, providers must go through an extensive and complex implementation process. Specifically, providers must perform an assessment of their existing processes and systems to determine what changes must be made; review, update, and negotiate supplier and other contracts; update written requirements documents; research, design, code, and test updates to customer care, self-serve, and back-office applications and systems; train employees and suppliers; draft customer communications; develop notice methods and periods; and set up a system for ensuring ongoing compliance. These actions will take a significant amount of time to complete, requiring approximately 18 months from the date rules are adopted.").

[57] § 64.2006(a).

[58] *Report and Order* ¶266.

details."[59] The Commission also established a "rebuttable presumption that any breach involving sensitive customer PI poses a reasonable likelihood of customer harm and would therefore require…notification."[60]

The Commission should recast the threshold for breach notification as the point at which a provider determines financial or physical harm is reasonably likely to occur, and that the person accessing customer data without authorization had the intent to use or share it. Without an intent element or other clear qualifiers, and without limiting the presumption that any sensitive customer PI triggers breach notices, the FCC will create an over-notification problem that will jeopardize consumer welfare and waste limited provider resources.[61] Generally speaking, asking a carrier to determine whether "emotional harm" is likely to occur, or adjudging whether a customer has "lost control" of their information is not reasonable, and cannot be practicably implemented as a matter of company policy. What is "emotionally harmful" to one person or group of people is varied and ambiguous, as well as what sort of breach may cause "reputational harm." An intent element would relieve the provider of contending with a highly subjective "reasonability" analysis regarding whether or not the requisite level of harm had occurred. Re-drafting the definition of breach to include an intent element, and a narrower set of

---

[59] *Id.*

[60] *Id.* ¶ 267. The FCC also dictates *when* carriers must notify consumers, the Commission and the Federal Bureau of Investigation ("FBI"). Once the breach notice requirements are implicated, a provider must notify affected consumers no later than 30 days after a breach; the content of the notice itself must include many details, including a description of the "customer PI that was breached or reasonably believed to have been breached."[60] The Commission must be notified of any breach affecting 5,000 or more customers within seven business days of occurrence, assuming no harm is reasonably likely to occur, and within 30 days if more than 5,000 customers are impacted.[60] The FBI and secret service will be notified for a breach affecting 5,000 or more customers, again assuming harm is reasonably likely to occur, within seven business days. *See id.*; *see also* § 64.2006(b).

[61] CCA Reply Comments at 16.

information, will rightly encourage easily-administrable data breach responses providing actual assistance to consumers.

Like the lack of intent, the Commission's blanket "presumption" that any breach of any sensitive customer PI is harmful and therefore triggers notice will overwhelm consumers with notices while simultaneously diminishing the impact of those notices.[62] Under the Commission's new rules, for example, breach of app data tracking hours of the Candy Crush game play could cost providers hundreds of thousands to comply with the *Report and Order*, even though the consumer has not been harmed. These rules are not in the public interest, as the FTC recognized that "notice fatigue" is an actual harm, stating that consumers could "become numb" to notices and may ignore of fail to recognize the risks detailed in the notice.[63]

Further, considering the vast resources which must be quickly deployed once the data notification requirements are set in motion, a higher trigger threshold is justified to preserve resources and ensure customers receive notice only as needed. Because this section of the *Report and Order* imposes substantive administrative and fact-finding burdens under an unreasonably short timeframe, it will not be easily approved by the Office of Management and Budget following the Paperwork Reduction Act review process. Small providers will be especially burdened by the date breach notice rules, and it is clear the Commission did not analyze what sort of strain a requirement to, for example, submit thousands of individual customer notices to the "email address or postal address…of the customer," will have on a small staff.[64]

---

[62] This "presumption" would perhaps be reasonable if the definition of "sensitive" information is consistent with the FTC regime.

[63] FTC Comments at 31.

[64] *See* § 64.2006(a)(1); *see also* CCA Reply Comments at 17-18, *citing* Draft NISTIR 7621 Revision 1, *Small Business Information Security: The Fundamentals*, Richard Kissel, Hyunjeong

The Commission should, at least, lengthen data breach notice timelines for small carriers.[65] The public interest is not served if customers are inundated with notices, where there is no reasonable expectation of harm at the hands of a bad faith actor. Thus, the Commission's definition of "breach" should be reconsidered.

Moon, U.S. Department of Commerce, 2 (December 2014) (asserting that the "average estimated cost for these notifications and associated security breach costs is well over $130 per person," equating to about $130,000 for a breach touching 1,000 consumers). CCA suggests holding small providers to an "as soon as practicable" notice standard with no less than 60 days total to issue notice of a harmful breach; small providers would reasonably be able to notify the FCC as well as the FBI and Secret Service of a harmful breach within 30 days.

[65] CCA Small Provider *Ex Parte* at 4.

IV. CONCLUSION

The Commission should not be able to initiate tectonic shifts in the way compliance resources are allocated unless it is firmly within its legal authority to do so, and the adopted rules are clearly designed to address real consumer injury. Therefore, reconsideration of the entire *Report and Order* is justified. However, if the FCC decides to review only specific provisions within the *Report and Order*, the Commission must reconsider rules that impose especially unreasonable burdens on BIAS providers without the counterbalancing benefit of proven consumer protection. Protecting small providers, and ensuring these community-rooted businesses are not forced to divert resources away from customer care or network maintenance and expansion, is critical. Further, adjusting the scope of information covered by the rules and retuning data breach rules helps to ensure that BIAS providers are on equal competitive footing with edge providers, promoting competition, innovation and clarity of consumer choice in the Internet ecosystem. The public interest is best served when entrepreneurial competitive carriers are focused on bringing faster and better services to their customers, not complying with voluminous federal regulations unconnected to concrete consumer harms.

Respectfully submitted,

/s/ Rebecca Murphy Thompson

Steven K. Berry
Rebecca Murphy Thompson
Elizabeth Barket
COMPETITIVE CARRIERS ASSOCIATION
805 15th Street NW, Suite 401
Washington, DC 20005

January 3, 2017